International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 11, Issue 2 (2025)
https://doi.org/10.31436/ijpcc.v11i2.528

Unified Secure Access Service Edge (SASE): Transforming Security for Hybrid Workforce and Multi-Cloud Environments

Zainab S. Attarbashi[1], Atikah Balqis Binti Basri[1] and Shayma Senan[2]

[1]department of Computer Science, International Islamic University Malaysia, Gombak, Malaysia.
[2]Electrical and Computer Engineering Department, International Islamic University Malaysia, Gombak, Malaysia.

*Corresponding author Zainab_senan@iium.edu.my
(Received: 19th December 2024; Accepted: 28th January, 2024; Published on-line: 30th July, 2025)

Abstract— Organizations increasingly adopt hybrid cloud infrastructures and hybrid workforce models, creating a demand for secure and seamless networking solutions. Unified Secure Access Service Edge (SASE) is an integrated architecture that combines wide-area networking (WAN) functionality with advanced network security, offering a unified solution to address these challenges. This article explores the key components of Unified SASE and their effectiveness in handling the complexities of cloud infrastructure adoption and hybrid work environment integration. By embedding security capabilities into a cloud-based framework, Unified SASE ensures rapid responses to evolving threats and facilitates consistent security policies across on-premise data centres and multi-cloud environments. This article emphasizes the importance of adhering to industry standards in the development and deployment of Unified SASE, particularly regarding compatibility and interoperability. Ultimately, Unified SASE addresses the challenges of cloud environments and hybrid workforce models by integrating network security with access services, providing enterprises with a robust framework for secure, efficient, and scalable operations.

Keywords— Unified SASE, hybrid cloud infrastructure, SD-WAN, Cloud Access Security Broker, Zero Trust Network Access.

I. Introduction

The rapid increase of digital transformation, cloud adoption, and remote work has created an urgent need for a more advanced and comprehensive networking and security model. Unified Secure Access Service Edge (SASE) [1] came as a transformative solution that integrates networking and security functionalities into a cloud-native architecture. By using these capabilities, organizations can enhance performance, strengthen security, simplify network management, and reduce complexity.

Traditional network architectures and security models are increasingly insufficient to address the demands of today's dynamic and distributed workforce. The dependence on appliance-centric security measures and perimeter-based strategies—characterized by data backhauling and fixed network perimeters—fails to meet the needs of environments driven by cloud-first and remote-work models. Unified SASE addresses these challenges by combining advanced networking technologies, such as Software-Defined Wide Area Networking (SD-WAN) [2], with comprehensive security features, including Zero Trust Network Access (ZTNA) [3], secure web gateways, cloud access security brokers (CASBs) [4], and firewall-as-a-service (FWaaS) [1]. By using a cloud-native approach, SASE creates a robust and scalable architecture that supports digital transformation, adapts to the growing number of endpoint devices, and meets the needs of hybrid and remote workforces.

This study highlights how unified SASE simplifies network management by merging multiple security services into a single platform by integrating services like data loss prevention (DLP) [5], secure web gateways, and firewall-as-a-service, ensuring consistent security policies across the entire network architecture while lowering operational costs.

Another critical aspect of this study is investigating how unified SASE enhances user experience and overall network performance. By using SD-WAN capabilities, organizations can optimize bandwidth utilization, reduce latency, and intelligently route traffic based on application priorities. This ensures optimal performance for critical business applications and seamless user experiences, regardless of user location or device. Furthermore, unified SASE's ability to dynamically allocate bandwidth based on business requirements enables enterprises to achieve greater efficiency and reliability in their network operations.

II. Technical Background

A. *Secure Access Service Edge (SASE) Architecture*

Secure Access Service Edge (SASE) has emerged as a transformative solution to address the complexities of secure communication across diverse business landscapes. By integrating network and security functionalities into a

https://doi.org/10.31436/ijpcc.v11i2.528

unified, cloud-native platform, SASE provides organizations with the tools to enhance security, streamline operations, and reduce complexity. Some of these integrated solutions are shown in figure 1:

- **Software-Defined Wide Area Networking (SD-WAN):** which intelligently manages network traffic across multiple connections, ensuring consistent performance and reliability. This capability enables seamless collaboration for geographically detached teams and ensures uninterrupted access to critical applications.
- **The Cloud Access Security Broker (CASB):** it empowers organizations with visibility and control over cloud services, enforcing strict data security policies and regulatory compliance. CASB mitigates risks by proactively safeguarding sensitive information stored in cloud environments.
- **Zero Trust Network Access (ZTNA):** focuses on validating user identities and authorizing access based on context rather than location. This approach minimizes the attack surface by granting access solely to authorized applications, replacing traditional VPN-based models with a more secure methodology. Zero Trust frameworks divide networks into smaller, isolated segments to reduce lateral movement of attackers by implementing a concept known as micro-segmentation. This approach creates distinct zones within the network, where each zone is isolated and protected by its own set of security policies.
- **Secure Web Gateways (SWG):** protects users from web-based threats by filtering malicious content.
- **Data Loss Prevention (DLP):** prevents unauthorized access or disclosure of sensitive data by enforcing robust security policies.
- **Firewall-as-a-Service (FWaaS):** provides traffic filtering and shields against unauthorized access, fortifying the network against evolving cyber threats and vulnerabilities.

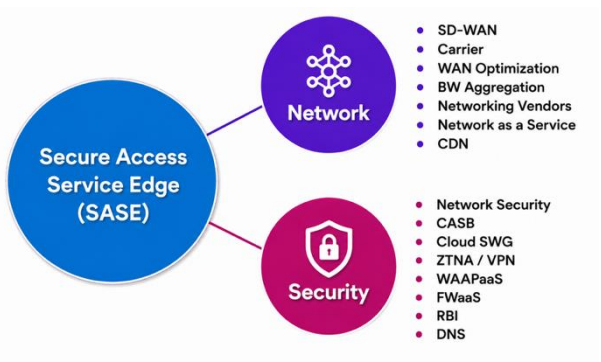

Fig 1. Technologies integrated in SASE

The adoption of SASE delivers many advantages, including simplified security management through the integration of multiple services into a unified platform that enables secure resource access from any location, improving user experiences and reducing costs by eliminating the need for disparate security solutions.

B. Unified Secure Access Service Edge (SASE)

Unified Secure Access Service Edge (Unified SASE) [6] improves SASE's foundational principles by combining security and networking functionalities into a single, streamlined cloud-based platform. This approach enhances operational efficiency and scalability, making it particularly valuable for enterprises with diverse and dynamic needs.

One of Unified SASE's core innovations is its single-pass scanning architecture, which inspects all network traffic only once. This design minimizes latency, reduces management complexity, and enhances performance while maintaining comprehensive visibility and control over network activities. This capability extends to advanced threat detection, including zero-day attacks and sophisticated malware. Figure 2 shows single pass parallel processing (SP3) architecture.

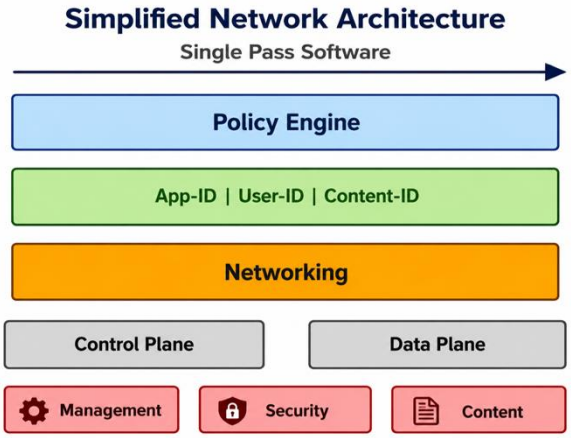

Fig 2. single pass parallel processing (SP3) architecture

A unified policy engine ensures consistent security policies across users, devices, and applications, regardless of their location. This reduces the administrative burden of managing disparate security systems. Additionally, centralized data storage in a unified data lake enables comprehensive insights into network activities, empowering organizations with real-time incident response and proactive security measures.

Unified SASE also provides a single solution for network management, simplifying operations, improving troubleshooting, and enhancing network health monitoring.

Table 1 shows a detailed comparison between SASE and Unified SASE.

TABLE I
COMPARISON BETWEEN SASE AND UNIFIED SASE

https://doi.org/10.31436/ijpcc.v11i2.528

Feature	SASE (Secure Access Service Edge)	Unified SASE
Definition	A framework that converges network and security services into a cloud-delivered model.	An enhanced and optimized version of SASE that integrates all components into a single architecture.
Core Components	- SD-WAN - ZTNA - CASB - SWG - FWaaS	All SASE components are unified into a single-pass architecture with optimized processing and management.
Architecture	Multi-vendor and fragmented deployment is common, often requiring separate platforms for network and security.	A single unified platform with integrated security and network functions managed centrally.
Data Processing	Security inspection may occur multiple times as data traverses different services (multi-pass inspection).	Single-pass inspection architecture processes traffic once for all security layers, reducing latency.
Policy Management	Policies are often spread across multiple systems, making management more complex.	Unified policy engine ensures consistent enforcement across all users, devices, and applications.
Deployment Flexibility	Often hybrid: mix of cloud-based and on-premise security solutions.	Fully cloud-native and scalable for global coverage with minimal dependency on on-premise hardware.
Scalability	Scalable but often limited by the multi-vendor approach.	Highly scalable due to unified architecture and centralized cloud-native platform.
Performance Optimization	SD-WAN optimizes traffic routing, but multi-pass inspection can cause performance issues.	Optimized traffic flow with single-pass scanning reduces latency and improves performance.
Visibility and Analytics	Disparate tools provide visibility; integrations may be required for holistic monitoring.	Unified data lake architecture provides centralized visibility and real-time analytics.
Threat Detection and Prevention	Each component handles threat detection individually, leading to inefficiencies.	Integrated threat intelligence, AI/ML-based analytics, and automated response enhance security.
Cost	Higher costs due to managing multiple solutions, vendors, and licenses.	Cost-efficient as it consolidates tools, and reduces hardware reliance.
Security Posture	Improved security but potentially inconsistent due to strict security services.	Enhanced security posture through integrated Zero Trust, consistent policies, and centralized controls.
Automation and AI Integration	Limited AI/ML usage across fragmented tools.	Advanced AI/ML capabilities enable automated threat detection, response, and optimization.
Vendor Lock-In	Can involve multiple vendors, reducing lock-in but increasing complexity.	Single-vendor solutions may increase lock-in but improve integration and support.

III. SASE in Hybrid Workforce Environments

The shift to hybrid work environments, where employees operate across remote and on-premises locations, has introduced unique security challenges. Organizations now face the critical task of safeguarding sensitive data, providing secure access to resources, and maintaining consistent performance across distributed workforces. Traditional perimeter-based security models, which rely on fixed network boundaries, are no longer effective in addressing the complexities of hybrid work setups. Vulnerabilities such as unsecured public Wi-Fi networks, the widespread use of personal devices, and the challenge of maintaining regulatory compliance further complicate the landscape.

Secure Access Service Edge (SASE) can play an important role in addressing these challenges by offering a unified, cloud-native framework that combines networking and security capabilities. With features like Zero Trust Network Access (ZTNA), SASE ensures access to corporate resources is granted based on identity, context, and policy, minimizing the risk of unauthorized access. Cloud-native security services deliver centralized protection to users and devices, whether they are working remotely or on-premises. Additionally, tools like Secure Web Gateway (SWG) and Cloud Access Security Broker (CASB) protect web traffic and cloud applications, enabling secure and seamless access for employees across different devices and locations. SD-WAN further enhances connectivity by optimizing traffic flow and ensuring consistent application performance, delivering a superior user experience.

In real-world scenarios, SASE has proven instrumental in supporting hybrid workforces. For example, a global consulting firm implemented SASE to secure remote access for employees using collaboration tools like Microsoft Teams and Google Workspace, enhancing productivity while maintaining robust security. Similarly, a healthcare provider adopted SASE to ensure HIPAA compliance [7], enabling doctors to securely access patient records from remote locations with the help of Data Loss Prevention (DLP) and CASB tools. In the retail sector, SASE has been used to secure both in-store point-of-sale systems and remote employee devices, while SD-WAN ensures optimal connectivity between branch locations and headquarters. Universities have also leveraged SASE to provide secure remote learning environments for students and faculty, ensuring access to internal systems without compromising security.

By integrating networking and security into a single framework, SASE empowers organizations to effectively support hybrid work environments. It provides enhanced security, seamless access, and optimized performance, enabling employees to remain productive and protected regardless of their location. This holistic approach ensures

https://doi.org/10.31436/ijpcc.v11i2.528

that hybrid workforces can adapt to evolving demands while maintaining operational resilience and data integrity.

IV. Unified SASE Applications

Unified Secure Access Service Edge (SASE) delivers a cloud-based solution for network security and connectivity. Its adaptability and robust feature set allow it to meet the unique security challenges and operational needs of various industries [8]. This section explores how Unified SASE provides solutions to address sector-specific challenges.

A) Healthcare

The healthcare industry faces many challenges, including protecting sensitive patient data, ensuring compliance with strict regulations, and supporting a distributed workforce of medical professionals [9]. Unified SASE provides a comprehensive and layered solution to address these challenges effectively.

1. **Strengthened Data Security:** Unified SASE ensures compliance with regulations such as HIPAA by implementing advanced security protocols. Zero Trust Network Access (ZTNA) minimizes vulnerabilities by verifying user identity and device context before granting access, thereby reducing the attack surface.
2. **Integrated Data Loss Prevention (DLP):** Unified SASE prevents data breaches by identifying and stopping unauthorized transmission of sensitive information. This proactive approach safeguards electronic health records (EHRs) and patient confidentiality.
3. **Robust Remote Access:** Unified SASE enables secure and reliable access to applications and patient data from any location, supporting critical healthcare functions. It ensures the continuity of telemedicine services, allowing uninterrupted patient care during disruptions such as natural disasters or pandemics. Additionally, it facilitates seamless collaboration among medical staff, regardless of their geographical location, enabling effective communication and data sharing. By reducing business interruptions and enhancing operational continuity, Unified SASE helps healthcare organizations maintain consistent and high-quality care delivery in dynamic and challenging environments.
4. **Simplified Management and AI-Driven Security:** A unified management console streamlines security administration, reduces IT workload, and improves operational efficiency. Unified SASE also leverages AI-powered threat detection and automated responses to minimize downtime and mitigate real-time cyber threats.
5. **Cost Optimization:** By integrating multiple security systems into a single framework, Unified SASE significantly reduces hardware and software maintenance costs as well as IT operational expenses. This streamlined approach allows healthcare organizations to optimize resources while enhancing overall efficiency. For example, Unified SASE empowers healthcare providers to balance robust data protection, secure access, and operational efficiency in an increasingly complex and dynamic environment.

B) Finance

Financial institutions are prime targets for cyberattacks and must adhere to strict regulatory requirements while maintaining high standards of service. Unified SASE provides a robust and integrated defence to ensure security, compliance, and operational efficiency [9]:

1. **Comprehensive Security and Fraud Prevention:** Unified SASE integrates key security features to provide comprehensive protection against cyber threats. These include web filtering, firewalls, and intrusion detection/prevention systems (IDPS), which work together to prevent unauthorized access and defend against cyberattacks. Additionally, Unified SASE leverages real-time threat intelligence, proactively identifying and mitigating risks to ensure adaptability to evolving cyber threats and maintaining a robust security posture.
2. **Regulatory Compliance:** Unified SASE simplifies compliance with industry standards such as PCI DSS through rigorous audit capabilities, consistent policy enforcement, and advanced reporting tools.
3. **Enhanced Customer Experience:** Unified SASE ensures secure and seamless access to critical financial applications, including online banking and trading platforms. It offers faster and more user-friendly authentication processes while maintaining robust transaction security, which fosters customer confidence and trust. These enhancements not only improve the user experience but also strengthen consumer trust, a vital factor in maintaining brand loyalty and enhancing the institution's reputation in a competitive financial landscape.
4. **Operational Efficiency and Scalability:** by automating routine security tasks, significantly reducing the manual workload for IT teams. Its cloud-native architecture provides seamless scalability, enabling financial organizations to quickly adapt to changing operational demands. It streamlines network and security management while eliminating redundant security systems, leading to reduced costs for software, hardware, and maintenance. This integrated approach not only optimizes resource utilization but also ensures that organizations remain robust in a dynamic business environment.

https://doi.org/10.31436/ijpcc.v11i2.528

C) Manufacturing

The manufacturing industry increasingly depends on interconnected systems such as Industrial IoT (IIoT), supply chain networks, and cloud platforms to drive operational efficiency and innovation. While these systems offer significant advantages, they also introduce vulnerabilities that require robust security measures. Unified SASE serves as an ideal solution by securing and optimizing these critical connections, ensuring seamless operation and data protection. Key Applications and Benefits:

1. **IIoT Security** [10]**:** Unified SASE provides comprehensive protection for smart factories and IoT devices, which are often the backbone of modern manufacturing processes. It safeguards these systems from cyber threats such as ransomware, unauthorized access, and network breaches. Features like Zero Trust Network Access (ZTNA) ensure that only authenticated users and devices can access IIoT networks, reducing the risk of malicious attacks.
2. **Supply Chain Visibility and Security:** Manufacturing organizations rely heavily on supply chain networks to manage logistics and inventory. Unified SASE secures access to cloud-based supply chain platforms, ensuring that data remains protected during transmission. This enables manufacturers to maintain real-time visibility into supply chain operations while safeguarding sensitive logistics information from cyber threats.
3. **Remote Monitoring and Maintenance:** With the increasing popularity of remote work, manufacturing engineers often need to access factory operations from remote locations. Unified SASE enables secure remote monitoring of machinery and processes, allowing engineers to diagnose issues, optimize workflows, and perform maintenance tasks without compromising security. This minimizes downtime and enhances overall productivity.
4. **Data Protection and Intellectual Property (IP) Security:** Unified SASE ensures the protection of sensitive data, including product designs, operational blueprints, and intellectual property (IP). Data Loss Prevention (DLP) features help prevent unauthorized sharing or exfiltration of critical information. By implementing centralized security policies, Unified SASE ensures consistent protection of valuable assets across distributed systems and locations.
5. **Performance Optimization:** Unified SASE's SD-WAN capabilities optimize network traffic, ensuring that critical applications such as IIoT platforms, analytics tools, and enterprise resource planning (ERP) systems receive priority bandwidth. This improves performance, reduces latency, and ensures smooth operation across distributed manufacturing sites.

Figure (3) summarize the applications of Unified SASE applications in different fields.

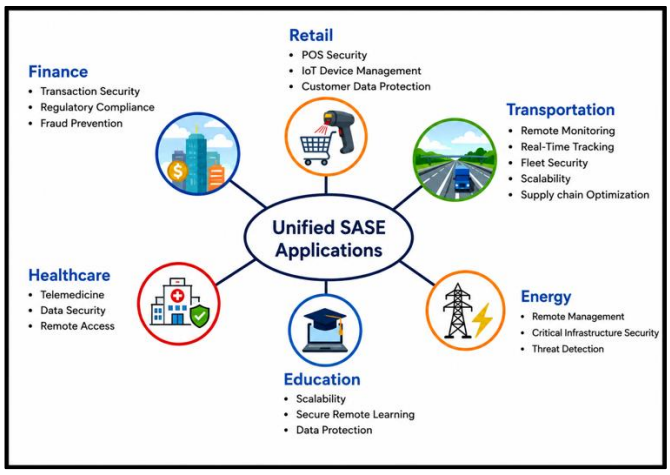

Fig 3. Unified SASE Applications

V. Challenges of Unified SASE Implementation

While Unified SASE provides many benefits, its implementation is not without challenges. Organizations, especially smaller ones, must carefully evaluate potential obstacles to ensure successful deployment and integration. Understanding these challenges is crucial for effective planning and execution.

One of the challenges lies in the significant initial investment required to adopt Unified SASE. For small and medium-sized enterprises, the transition to a cloud-native architecture may involve replacing or upgrading legacy infrastructure, subscribing to comprehensive SASE solutions, and selecting the appropriate vendor for their specific needs. While larger enterprises may find it easier to allocate resources, small enterprises often struggle to justify the costs, especially if their existing systems are still functional. The subscription-based pricing models of many SASE platforms further add to ongoing operational costs, making affordability a key concern for smaller organizations.

Organizations must also address technical challenges such as configuring legacy hardware to work with software-defined perimeters or ensuring that older applications can communicate effectively with centralized SASE frameworks. Additionally, migrating from legacy systems to SASE without disrupting ongoing operations can be a complex and resource-intensive process, requiring careful planning and phased implementation to mitigate risks.

The successful adoption of Unified SASE also depends heavily on the readiness of IT teams to manage its advanced features. Many organizations face a skills gap, as existing teams may not have expertise in managing components

https://doi.org/10.31436/ijpcc.v11i2.528

such as ZTNA, SWG, and centralized policy engines. Furthermore, adjusting to new workflows, such as monitoring and managing a single-pane-of-glass interface, can initially create operational inefficiencies. Without adequate preparation, there is a risk of misconfigurations, which can compromise the security and performance of the framework.

VI. Future Directions in Unified SASE Technology

The evolution of Unified SASE technology continues to redefine network security and connectivity, driven by emerging trends and advancements in AI/ML integration. One key trend is the shift towards greater automation and intelligence in SASE frameworks, where AI and machine learning (ML) are increasingly being utilized for predictive security [10]. Machine learning models are trained using large datasets comprising malware signatures, behavioural patterns, and network traffic anomalies. Supervised learning techniques are applied to identify specific attack patterns, while unsupervised learning detects anomalies that deviate from baseline behaviours.

TABLE III
TRAINING MACHINE LEARNING MODELS FOR THREAT DETECTION

	Supervised Learning	**Unsupervised Learning**	**Reinforcement Learning**
Purpose	Identifies specific attack patterns using labelled datasets of known threats.	Detects anomalies by analysing deviations from baseline behaviours.	Learns optimal responses to threats through trial-and-error and feedback.
Training Data	Requires labelled data with predefined categories (e.g., malicious vs. non-malicious).	Relies on unlabelled data to uncover hidden patterns and irregularities.	Uses real-time interaction data and rewards to refine decision-making.
Use Cases	Effective for detecting known threats (e.g., malware signatures).	Ideal for identifying zero-day exploits and previously unseen attack vectors.	Useful for dynamically adapting to evolving attack strategies over time.
Detection Mechanism	Matches inputs against pre-trained patterns or signatures.	Flags deviations from established normal behaviour as potential threats.	Develops policies to take proactive actions in uncertain environments.
Advantages	High accuracy for known threats; quick deployment if labelled data is available.	Capable of identifying new or emerging threats without prior knowledge.	Continuously improves detection capabilities in dynamic, real-world settings.
Challenges	Requires a large, labelled dataset; less effective for unknown threats.	May generate false positives due to lack of predefined attack patterns.	Requires significant computational resources and training time.

By analysing huge amounts of network data in real time, AI/ML algorithms can identify potential threats before they happen, enabling proactive responses and reducing the risk of breaches. This capability is particularly valuable in detecting sophisticated attacks such as zero-day exploits and advanced persistent threats (APTs). Table highlights different approaches to training machine learning models for threat detection.

Another significant direction is the growing emphasis on integrating Unified SASE with emerging network architectures such as 5G, edge computing, and hybrid cloud environments. These advancements demand scalable, low-latency solutions, which SASE is uniquely positioned to deliver through its unified and cloud-native framework. As organizations adopt distributed architectures, SASE will play a critical role in ensuring seamless connectivity and security across diverse endpoints and geographies.

Additionally, the evolution of security paradigms continues to influence SASE development. The adoption of Zero Trust principles, combined with enhanced policy enforcement capabilities, is expected to further strengthen organizational defences against evolving threats. The increasing reliance on decentralized workforces and IoT devices highlights the need for flexible, adaptable solutions like Unified SASE, which can dynamically adjust to changing environments without compromising performance.

VII. CONCLUSION

The Unified Secure Access Service Edge (Unified SASE) is a transformative solution for organizations adapting to hybrid cloud infrastructures and remote work models. By integrating wide-area network (WAN) functions with advanced network security features, Unified SASE addresses challenges associated with cloud adoption and hybrid work environments. Its focus on threat prevention, data protection, and secure user experiences ensures consistent security and productivity across various deployment scenarios. Unified SASE's scalability and adherence to industry standards ensure compatibility and interoperability, making it a robust framework for modern organizational needs. It empowers hybrid workforces, secures branch and retail locations, supports cloud and digital transformation initiatives, and enhances digital forensic readiness. These capabilities highlight its role in aligning security strategies with evolving operational demands. Overall, Unified SASE provides a robust and adaptive architecture that enables organizations to build resilient, future-proof networks, meeting the demands of today's dynamic corporate landscape.

ACKNOWLEDGMENT

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took their time to study the manuscript and find it acceptable for publishing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest

REFERENCES

[1] M. Wood, "How SASE is defining the future of network security," Network Security, vol. 2020, no. 12, pp. 6–8, Dec. 2020, doi: 10.1016/S1353-4858(20)30139-2.

[2] J. Wang, M. Bewong, and L. Zheng, "SD-WAN: Hybrid Edge Cloud Network between Multi-site SDDC," Computer Networks, vol. 250, p. 110509, Aug. 2024, doi: 10.1016/j.comnet.2024.110509.

[3] O. Lamdakkar, I. Ameur, M. M. Eleyatt, F. Carlier, and L. A. Ibourek, "Toward a modern secure network based on next-generation firewalls: recommendations and best practices," Procedia Comput Sci, vol. 238, pp. 1029–1035, 2024, doi: 10.1016/j.procs.2024.06.130.

[4] S. S. Chauhan, E. S. Pilli, R. C. Joshi, G. Singh, and M. C. Govil, "Brokering in interconnected cloud computing environments: A survey," J Parallel Distrib Comput, vol. 133, pp. 193–209, Nov. 2019, doi: 10.1016/j.jpdc.2018.08.001.

[5] S. Ahmad, S. Mehfuz, and J. Beg, "Cloud security framework and key management services collectively for implementing DLP and IRM," Mater Today Proc, vol. 62, pp. 4828–4836, 2022, doi: 10.1016/j.matpr.2022.03.420.

[6] M. Giess, "CPaaS and SASE: the best defences against IoT threats," Network Security, vol. 2021, no. 9, pp. 9–12, Sep. 2021, doi: 10.1016/S1353-4858(21)00103-3.

[7] B. C. Drolet, J. S. Marwaha, B. Hyatt, P. E. Blazar, and S. D. Lifchez, "Electronic Communication of Protected Health Information: Privacy, Security, and HIPAA Compliance," J Hand Surg Am, vol. 42, no. 6, pp. 411–416, Jun. 2017, doi: 10.1016/j.jhsa.2017.03.023.

[8] R. Chen, S. Yue, W. Zhao, M. Fei, and L. Wei, "Overview of the Development of Secure Access Service Edge," 2023, pp. 138–145. doi: 10.1007/978-981-19-9968-0_17.

[9] M. N. Islam, R. Colomo-Palacios, and S. Chockalingam, "Secure Access Service Edge: A Multivocal Literature Review," in 2021 21st International Conference on Computational Science and Its Applications (ICCSA), IEEE, Sep. 2021, pp. 188–194. doi: 10.1109/ICCSA54496.2021.00034.

[10] A. Houkan et al., "Enhancing Security in Industrial IoT Networks: Machine Learning Solutions for Feature Selection and Reduction," IEEE Access, vol. 12, pp. 160864–160883, 2024, doi: 10.1109/ACCESS.2024.3481459.